syslogを管理します

SANtricity software

NetApp
March 27, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/e-series-santricity-117/sm-settings/view-audit-log-activity.html on March 27, 2025. Always check docs.netapp.com for the latest.

目次

syslogを管理します 1
- 監査ログアクティビティを表示します 1
- 監査ログポリシーを定義する 3
- 監査ログからイベントを削除します 4
- 監査ログ用のsyslogサーバを設定します 5
- 監査ログレコード用のsyslogサーバ設定の編集 6

syslogを管理します

監査ログアクティビティを表示します

Security Admin権限を持つユーザは、監査ログを表示して、ユーザによる操作、認証エラー、無効なログインの試行、およびユーザセッションの期間を監視できます。

作業を開始する前に

Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

手順

1. メニューを選択します。Settings [Access Management]。
2. [監査ログ]タブを選択します。

   監査ログアクティビティが表形式で表示されます。各列に表示される情報は次のとおりです。

   - 日付/時刻--ストレージアレイがイベントを検出した日時（GMT）のタイムスタンプ
   - ユーザー名--イベントに関連付けられたユーザー名。ストレージアレイに対して認証されていない操作が実行された場合は、「N/A」と表示されます。内部プロキシまたはその他のメカニズムによって、認証されていないアクションがトリガーされることがあります。
   - ステータスコード--操作のHTTPステータスコード(200、400など)およびイベントに関連する説明テキスト。
   - **URL**アクセス--完全なURL (ホストを含む)とクエリ文字列。
   - クライアント**IP**アドレス--イベントに関連付けられたクライアントのIPアドレス。
   - **Source**--イベントに関連付けられたロギングソース。System Manager、CLI、Webサービス、またはサポートシェルがあります。
   - *概要 *--イベントに関する追加情報 （該当する場合）。
3. [監査ログ]ページの選択項目を使用して、イベントを表示および管理します。

選択の詳細

選択（**Selection**）	説明
イベントを表示する期間を選択…	表示されるイベントを日付範囲（過去24時間、過去7日間、過去30日間、またはカスタムの日付範囲）で限定します。
フィルタ	表示されるイベントをフィールドに入力した文字で限定します。完全に一致する単語には引用符（""）を使用し、次のように入力します。 `OR` 1つまたは複数の単語を返すには、ダッシュ（--）を入力して単語を省略します。
更新	最新のイベントにページを更新するには、「更新」を選択します。
設定の表示/編集	［表示/設定の編集］を選択すると、ログに記録するフルログポリシーとアクションのレベルを指定できるダイアログボックスが開きます。
イベントを削除します	「削除」を選択すると、ページから古いイベントを削除できるダイアログボックスが開きます。
列の表示/非表示を切り替えます	[列を表示/非表示（* Show/Hide * Column）]アイコンをクリックします をクリックして、表に表示する列を追加で選択します。 その他の列には、次のもの • メソッド-- HTTPメソッド(POST、GET、削除など)。 • **CLI**コマンド実行-- Secure CLI要求に対して実行されるCLIコマンド(文法)。 • **CLI**戻りステータス-- CLIステータスコードまたはクライアントからの入力ファイルの要求。 • *SYMBOL手順 *--実行されたSYMBOL手順 。 • *SSH Event Type *-- Secure Shell (SSH)イベントのタイプ(ログイン、ログアウト、login_failなど) • *SSHセッションPID *-- SSHセッションのプロセスID番号。 • **SSH**セッション期間--ユーザーがログインした秒数 • 認証タイプ--ローカルユーザー、LDAP、SAML、およびアクセストークンを含むことができます。 • *認証ID *--認証されたセッションのID。
列フィルタを切り替えます	[切り替え*（Toggle *）]アイコンをクリックします をクリックすると、各列のフィルタリングフィールドが開きます。 表示されるイベントを特定の文字で限定するには、列フィールドにその文字を入力します。フィルタリングフィールドを閉じるには、アイコンをもう一度クリックします。

選択（**Selection**）	説明
変更を元に戻します	[元に戻す（Undo）]アイコンをクリックします をクリックすると、テーブルがデフォルトの設定に戻ります。
エクスポート（Export）	[**Export**]をクリックして、テーブルデータをカンマ区切り値（CSV）ファイルに保存します。

監査ログポリシーを定義する

上書きポリシーや監査ログに記録するイベントのタイプを変更することができます。

作業を開始する前に

Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

このタスクについて

このタスクでは、監査ログの設定を変更する方法について説明します。古いイベントの上書きに関するポリシーや記録するイベントタイプに関するポリシーなどが含まれます。

手順

1. メニューを選択します。Settings [Access Management]。
2. [監査ログ]タブを選択します。
3. 「表示/設定の編集」を選択します。

   [監査ログの設定]ダイアログボックスが開きます。
4. 上書きポリシーや記録するイベントのタイプを変更します。

フィールドの詳細

設定	説明
上書きポリシー	最大容量に達したときに古いイベントを上書きするポリシーを指定します。 • 監査ログがいっぱいになったらイベントを古いものから上書きする-監査ログが50、000レコードに達したときに古いイベントを上書きします。 • 監査ログのイベントを手動で削除する必要があります-イベントが自動的に削除されないように指定します。設定した割合に達した場合、しきい値の警告が表示されます。イベントは手動で削除する必要があります。 上書きポリシーを無効にした場合、監査ログのエントリが上限に達すると、Security Adminの権限がないユーザによるSystem Managerへのアクセスは拒否されます。Security Adminの権限がないユーザが再びシステムにアクセスできるようにするには、Security Adminロールが割り当てられているユーザが古いイベントレコードを削除する必要があります。 上書きポリシーは、監査ログをsyslogサーバにアーカイブするように設定されている場合は適用されません。
ログに記録するアクションのレベル	ログに記録するイベントのタイプを指定します。 • 変更イベントのみを記録する--ユーザーの操作によってシステムに変更が発生するイベントのみを記録します • すべての変更イベントと読み取り専用イベントを記録する--情報の読み取りまたはダウンロードを伴うユーザー操作を含むすべてのイベントを記録します

5. [保存（ Save ）] をクリックします。

監査ログからイベントを削除します

監査ログの古いイベントをクリアすることができます。これにより、イベントの検索が容易になります。削除時に古いイベントをCSV（カンマ区切り値）ファイルに保存することもできます。

作業を開始する前に

Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。

手順

1. メニューを選択します。Settings [Access Management]。
2. [監査ログ]タブを選択します。
3. 「 * 削除」を選択します。

   Delete Audit Logダイアログボックスが開きます。

4. 削除する古いイベントの数を選択または入力します。
5. 削除したイベントをCSVファイルにエクスポートする場合は、チェックボックスを選択したままにします（推奨）。次の手順で*削除*をクリックすると、ファイル名と場所の入力を求められます。イベントをCSVファイルに保存しない場合は、チェックボックスをクリックして選択を解除します。
6. [削除（ Delete ）] をクリックします。

   確認のダイアログボックスが開きます。

7. を入力します `delete` フィールドで、*[削除]*をクリックします。

   最も古いイベントは監査ログページから削除されます。

監査ログ用の**syslog**サーバを設定します

監査ログを外部のsyslogサーバにアーカイブする場合は、そのサーバとストレージアレイの間の通信を設定できます。接続が確立されると、監査ログは自動的にsyslogサーバに保存されます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- syslogサーバのアドレス、プロトコル、およびポート番号を確認しておく必要があります。サーバアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- サーバがセキュアなプロトコル（TLSなど）を使用している場合は、ローカルシステムに認証局（CA）証明書が配置されている必要があります。CA証明書がWebサイトの所有者を識別することにより、サーバとクライアントの間のセキュアな接続が確立さ

手順

1. メニューを選択します。Settings [Access Management]。
2. 監査ログタブで、*Configure Syslog Servers *を選択します。

   Configure Syslog Serversダイアログボックスが開きます。

3. [追加（ Add ）] をクリックします。

   [Add Syslog Server]ダイアログボックスが開きます。

4. サーバーの情報を入力し、*追加*をクリックします。
   - サーバーアドレス--完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを入力します。

- **Protocol**--ドロップダウンリストからプロトコル(TLS、UDP、TCPなど)を選択します。
- 証明書のアップロード（オプション）-- TLSプロトコルを選択して署名済みCA証明書をまだアップロードしていない場合は、[*参照]をクリックして証明書ファイルをアップロードします。監査ログは、信頼された証明書がないとsyslogサーバにアーカイブされません。

> あとで証明書が無効になると、TLSハンドシェイクは失敗します。その結果、監査ログにエラーメッセージが記録され、syslogサーバにメッセージが送信されなくなります。この問題 を解決するには、syslogサーバで証明書を修正してから、メニューの[設定]、[監査ログ]、[syslogサーバの設定]、[すべてテスト]の順に選択します。

- ポート-- syslogレシーバーのポート番号を入力します。 [Add *]をクリックすると、[Configure Syslog Servers]ダイアログボックスが開き、設定したsyslogサーバがページに表示されます。

5. ストレージアレイとのサーバ接続をテストするには、「*すべてテスト」を選択します。

結果

設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。

監査ログレコード用のsyslogサーバ設定の編集

監査ログのアーカイブに使用するsyslogサーバの設定を変更したり、サーバ用の新しい認証局（CA）証明書をアップロードしたりできます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- syslogサーバのアドレス、プロトコル、およびポート番号を確認しておく必要があります。サーバアドレスは、完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスのいずれかで指定できます。
- 新しいCA証明書をアップロードする場合は、ローカルシステムに証明書がある必要があります。

手順

1. メニューを選択します。Settings [Access Management]。
2. 監査ログタブで、*Configure Syslog Servers *を選択します。

   設定されているsyslogサーバがページに表示されます。

3. サーバ情報を編集するには、サーバ名の右側にある* Edit *（鉛筆）アイコンを選択し、次のフィールドで必要な変更を行います。
   - サーバーアドレス--完全修飾ドメイン名、IPv4アドレス、またはIPv6アドレスを入力します。
   - **Protocol**--ドロップダウンリストからプロトコル(TLS、UDP、TCPなど)を選択します。
   - ポート-- syslogレシーバーのポート番号を入力します。
4. （UDPまたはTCPから）プロトコルをセキュアTLSプロトコルに変更した場合は、[**Import Trusted Certificate**]をクリックしてCA証明書をアップロードします。
5. ストレージアレイとの新しい接続をテストするには、「*すべてテスト」を選択します。

結果

設定が完了すると、以降すべての監査ログがsyslogサーバに送信されるようになります。以前のログは転送されません。

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。